Detecting False Data Injection Attacks in Smart Grids: A Semi-Supervised Deep Learning Approach

Year: 2021 | Citations: 239 | Authors: Ying Zhang, Jianhui Wang, Bo Chen

Abstract

The dependence on advanced information and communication technology increases the vulnerability in smart grids under cyber-attacks. Recent research on unobservable false data injection attacks (FDIAs) reveals the high risk of secure system operation, since these attacks can bypass current bad data detection mechanisms. To mitigate this risk, this paper proposes a data-driven learning-based algorithm for detecting unobservable FDIAs in distribution systems. We use autoencoders for efficient dimension reduction and feature extraction of measurement datasets. Further, we integrate the autoencoders into an advanced generative adversarial network (GAN) framework, which successfully detects anomalies under FDIAs by capturing the unconformity between abnormal and secure measurements. Also, considering that the datasets collected from practical power systems are partially labeled due to expensive labeling costs and missing labels, the proposed method only requires a few labeled measurement data in addition to unlabeled data for training. Numerical simulations in three-phase unbalanced IEEE 13-bus and 123-bus distribution systems validate the detection accuracy and efficiency of this method.